

PATENT ABSTRACTS OF JAPAN

(11)Publication number : 2002-055955

(43)Date of publication of application : 20.02.2002

(51)Int.Cl.

G06F 15/00

H04Q 7/38

H04L 9/32

H04M 3/42

(21)Application number : 2000-238517

(71)Applicant : DOCOMO SYSTEMS INC

(22)Date of filing : 07.08.2000

(72)Inventor : KAWASHIMA OSAMU

NODA HIROTO

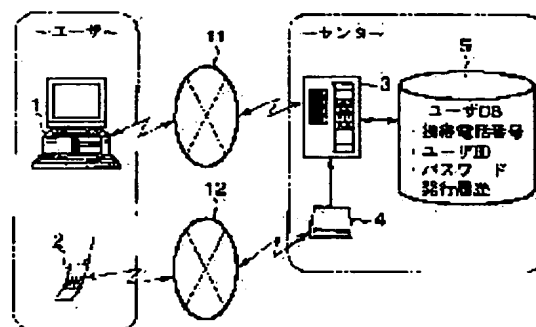
KAZUNO AKIRA

(54) METHOD AND SYSTEM FOR PERSONAL AUTHENTICATION

(57)Abstract:

PROBLEM TO BE SOLVED: To provide a method and a system for personal authentication with superior security, which can eliminate unauthorized access by a 3rd party as much as possible.

SOLUTION: A user ID, a password, a telephone number for authentication, and a caller telephone number are used as elements for authenticating a registered person. The user ID and caller telephone number are previously registered and the password and telephone number for authentication are issued by a server 3 when the server is accessed.



LEGAL STATUS

[Date of request for examination]

07.08.2000

[Date of sending the examiner's decision of rejection]

[Kind of final disposal of application other than the examiner's decision of rejection or application converted registration]

[Date of final disposal for application]

[Patent number]

3479634

[Date of registration]

03.10.2003

[Number of appeal against examiner's decision of rejection]

[Date of requesting appeal against examiner's
decision of rejection]

[Date of extinction of right]

(19)日本国特許庁 (J P)

(12) 公開特許公報 (A)

(11)特許出願公開番号
特開2002-55955
(P2002-55955A)

(43)公開日 平成14年2月20日(2002.2.20)

| (51)IntCl. ⁷ | 識別記号 | F I | テーマコード*(参考) | |
|-------------------------|-------|---------------|-------------|-----------|
| G 0 6 F 15/00 | 3 3 0 | G 0 6 F 15/00 | 3 3 0 B | 5 B 0 8 5 |
| | | | 3 3 0 C | 5 J 1 0 4 |
| H 0 4 Q 7/38 | | H 0 4 M 3/42 | E | 5 K 0 2 4 |
| H 0 4 L 9/32 | | H 0 4 B 7/26 | 1 0 9 R | 5 K 0 6 7 |
| H 0 4 M 3/42 | | H 0 4 L 9/00 | 6 7 3 A | |

審査請求 有 請求項の数 3 O L (全 5 頁) 最終頁に続く

(21)出願番号 特願2000-238517(P2000-238517)

(22)出願日 平成12年8月7日(2000.8.7)

(71)出願人 591144475

ドコモ・システムズ株式会社
東京都品川区西五反田四丁目31番18号

(72)発明者 川島 攻

東京都品川区西五反田四丁目31番18号 ア
イ・エヌ・エス・エンジニアリング株式会
社内

(72)発明者 野田 浩人

東京都品川区西五反田四丁目31番18号 ア
イ・エヌ・エス・エンジニアリング株式会
社内

(74)代理人 100058479

弁理士 鈴江 武彦 (外5名)

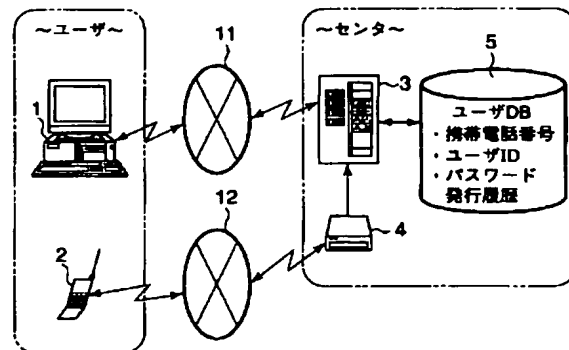
最終頁に続く

(54)【発明の名称】 本人認証方法および本人認証システム

(57)【要約】

【課題】 第三者による不正なアクセスを極力排除することができるセキュリティ性にすぐれた本人認証方法および本人認証システムを提供できる。

【解決手段】 登録者本人を認証する要素として、ユーザID、パスワード、認証用電話番号、発信者電話番号を使用する。ユーザIDおよび発信者電話番号は予め登録され、パスワードおよび認証用電話番号はアクセス時にサーバ3から発行される。



【特許請求の範囲】

【請求項1】 端末からのアクセスに際し同端末で入力される識別情報と予め登録されている識別情報とを照合するステップと、

この照合結果が一致の場合に、任意のパスワードを特定の認証用電話番号と共にアクセス元の端末に送信するステップと、

前記認証用電話番号に基づく電話回線接続を受けた場合にその電話の発信者番号を識別するステップと、

この識別された発信者番号と予め登録されている発信者番号とを照合するステップと、

この照合結果が一致の場合に、アクセス元の端末または電話回線接続の発信元に対しパスワードの入力を要求するステップと、

この要求後、アクセス元の端末または電話回線接続の発信元で入力されるパスワードと前記送信済みのパスワードとを照合するステップと、

この照合結果が一致の場合に、前記端末からのアクセス者が登録者本人であることを認証するステップと、を備えたことを特徴とする本人認証方法。

【請求項2】 情報入力用の端末と、所定のネットワークアドレスが設定され、前記端末からのネットワークを介したアクセスおよび外部からの電話回線による接続が可能な処理装置と、この処理装置に設けられ、前記端末からのアクセスに際し同端末で入力される識別情報と予め登録されている識別情報とを照合し、この照合結果が一致の場合に、任意のパスワードを前記電話回線による接続のための認証用電話番号と共にアクセス元の端末に送信する第1制御手段と、

前記認証用電話番号に基づいて前記処理装置への電話回線接続があった場合にその電話の発信者番号を識別する識別手段と、

前記処理装置に設けられ、前記識別手段の識別結果と予め登録されている発信者番号とを照合し、この照合結果が一致の場合に、アクセス元の端末または電話回線接続の発信元に対しパスワードの入力を要求する第2制御手段と、

前記処理装置に設けられ、アクセス元の端末または電話回線接続の発信元で入力されるパスワードと前記送信済みのパスワードとを照合し、この照合結果が一致の場合に、前記端末からのアクセス者が登録者本人であることを認証する第3制御手段と、を具備したことを特徴とする本人認証システム。

【請求項3】 請求項2に記載の本人認証システムにおいて、

前記電話回線は、携帯電話器による通信が可能な無線電話回線であることを特徴とする本人認証システム。

【発明の詳細な説明】

【0001】

【発明の属する技術分野】この発明は、ネットワークを介したサービス提供などに用いられる本人認証方法および本人認証システムに関する。

【0002】

【従来の技術】ネットワークを介したサービス提供たとえばオンラインショッピングでは、端末としてパーソナルコンピュータが使用され、サービスを提供する側の処理装置としてサーバコンピュータ（以下、サーバと略称する）が使用される。

【0003】サーバにはユーザ（利用者）の識別情報いわゆるユーザIDが予め登録され、パーソナルコンピュータからのアクセスに際し、ユーザは自身のユーザIDを入力することになる。この入力されるユーザIDと登録済みのユーザIDとが照合され、両者が一致する場合のみ、サーバでのサービス提供が許可される。

【0004】

【発明が解決しようとする課題】ユーザに与えられるユーザIDは、第三者に漏れることがある。ユーザIDが第三者に知られると、第三者がサーバにアクセスしてサービスを受けることが可能となり、まったく覚えのない商品の代金が正規のユーザに請求されるなど、正規のユーザに被害が及ぶことがある。これは、ユーザだけでなく、サービスを提供する側の業者にとっても、大きな問題となっている。

【0005】この発明は上記の事情を考慮したもので、その目的とするところは、第三者による不正なアクセスを極力排除することができるセキュリティ性にすぐれた本人認証方法および本人認証システムを提供することにある。

【0006】

【課題を解決するための手段】請求項1に係る発明の本人認証方法は、端末からのアクセスに際し同端末で入力される識別情報と予め登録されている識別情報とを照合するステップと、この照合結果が一致の場合に、任意のパスワードを特定の認証用電話番号と共にアクセス元の端末に送信するステップと、上記認証用電話番号に基づく電話回線接続を受けた場合にその電話の発信者番号を識別するステップと、この識別された発信者番号と予め登録されている発信者番号とを照合するステップと、この照合結果が一致の場合に、アクセス元の端末または電話回線接続の発信元に対しパスワードの入力を要求するステップと、この要求後、アクセス元の端末または電話回線接続の発信元で入力されるパスワードと上記送信済みのパスワードとを照合するステップと、この照合結果が一致の場合に、上記端末からのアクセス者が登録者本人であることを認証するステップと、を備えている。

【0007】請求項2に係る発明の本人認証システムは、情報入力用の端末と、所定のネットワークアドレスが設定され、上記端末からのネットワークを介したアクセスおよび外部からの電話回線による接続が可能な処理

装置と、この処理装置に設けられ、上記端末からのアクセスに際し同端末で入力される識別情報と予め登録されている識別情報とを照合し、この照合結果が一致の場合に、任意のパスワードを上記電話回線による接続のための認証用電話番号と共にアクセス元の端末に送信する第1制御手段と、上記認証用電話番号に基づいて上記処理装置への電話回線接続があった場合にその電話の発信者番号を識別する識別手段と、上記処理装置に設けられ、上記識別手段の識別結果と予め登録されている発信者番号とを照合し、この照合結果が一致の場合に、アクセス元の端末または電話回線接続の発信元に対しパスワードの10 入力を要求する第2制御手段と、上記処理装置に設けられ、アクセス元の端末または電話回線接続の発信元で入力されるパスワードと上記送信済みのパスワードとを照合し、この照合結果が一致の場合に、上記端末からのアクセス者が登録者本人であることを認証する第3制御手段と、を備えている。

【0008】請求項3に係る発明の本人認証システムは、請求項2に係る発明において、電話回線について限定している。電話回線は、携帯電話器用の無線電話回線20 である。

【0009】

【発明の実施の形態】以下、この発明の一実施形態について図面を参照して説明する。

【0010】図1に示すように、情報入力用の端末として、ユーザ宅にパーソナルコンピュータ1が設置されている。2は携帯電話器で、ユーザが専用に所持している。

【0011】一方、処理装置として、管理センタにサーバコンピュータ（以下、サーバと略称する）3が設置されている。サーバ3には所定のネットワークアドレスが設定されており、このネットワークアドレスに基づき、上記パーソナルコンピュータ1からサーバ3へのネットワーク11を介したアクセスが可能となっている。

【0012】また、サーバ3は、特定の認証用電話番号に基づいて、外部からの電話回線接続を受付ける機能を備えている。すなわち、上記携帯電話器2から特定の認証用電話番号を入力することにより、その携帯電話器2とサーバ3とが無線電話回線（デジタル電話回線、携帯電話網とも称す）12を介して相互接続される。

【0013】さらに、サーバ3に対し、発信者番号受信装置（識別手段）4およびユーザデータベース（以下、ユーザDBと略称する）5が接続されている。

【0014】発信者番号受信装置4は、サーバ3への電話回線接続があった場合に、その電話から発せられるデータを受信し、そのデータに基づいて同電話の発信者番号（例えば携帯電話番号）を識別する。

【0015】ユーザDB5には、登録を許可された者だけに与えられる識別情報いわゆるユーザID（加入者IDとも称す）が登録されるとともに、その登録者が所持

している携帯電話番号（または自宅電話番号）が発信者電話番号としてユーザIDに対応付ける形で登録され、さらに、後述のパスワード発行履歴が逐次に追加記憶される。

【0016】そして、サーバ3は、たとえばネットワークショッピングのサービスを提供するためのホームページ画像情報を内部メモリに有するとともに、主要な機能として次の[1]～[4]を有している。

【0017】[1] パーソナルコンピュータ1からのアクセスに際し、同パーソナルコンピュータ1で入力されるユーザIDとユーザDB5に登録されているユーザIDとを照合し、この照合結果が一致の場合に、任意のパスワードをランダムに選定し、そのパスワードをユーザIDに対応付けた形のパスワード発行履歴としてユーザDB5に記憶するとともに、同パスワードを電話回線接続用の特定の認証用電話番号と共にアクセス元のパーソナルコンピュータ1に送信する第1制御手段。

【0018】[2] 発信者番号受信装置4で識別された発信者番号とユーザDB5に登録されている発信者番号とを照合し、この照合結果が一致の場合に、アクセス元のパーソナルコンピュータ1または電話回線接続の発信元に対しパスワードの入力を要求する第2制御手段。

【0019】[3] アクセス元のパーソナルコンピュータ1または電話回線接続の発信元から入力されるパスワードと上記送信済みのパスワード（ユーザDB5内のパスワード発行履歴）とを照合し、この照合結果が一致の場合に、パーソナルコンピュータ1からのアクセス者が登録者本人であることを認証する第3制御手段。

【0020】[4] アクセス者が登録者本人であることを認証したとき、パーソナルコンピュータ1からのアクセスに応じたネットワークショッピングのサービスの提供を許可する第4制御手段。

【0021】つぎに、上記の構成の作用を図2を参照しながら説明する。ネットワークショッピングのサービスを受けようとするユーザが自宅のパーソナルコンピュータ1でサーバ3のネットワークアドレスを入力すると、パーソナルコンピュータ1がネットワーク11を介してサーバ3に接続される。この状態で、ユーザがパーソナルコンピュータ1からユーザIDを入力すると、そのユーザIDとユーザDB5に登録されているユーザIDとが照合される。

【0022】ユーザIDの照合が不一致の場合、アクセス者が登録ユーザではないとの判断の下に、アクセス拒否通知（文字データ）がサーバ3からパーソナルコンピュータ1に送られる。

【0023】ユーザIDの照合が一致の場合、サーバ3において任意のパスワードがランダムに選定され、そのパスワードがパスワード発行履歴の形でユーザDB5に記憶されるとともに、同パスワードが認証用電話番号と共にアクセス元のパーソナルコンピュータ1に送信され

る。送信されたパスワードおよび認証用電話番号は、パーソナルコンピュータ1のディスプレイで表示される。

【0024】ユーザは、ディスプレイを見てパスワードおよび認証用電話番号を確認し、そのうちの認証用電話番号を自身の携帯電話器2で入力する。すると、携帯電話器2とサーバ3とが無線電話回線12を介して接続され、その接続に伴い、携帯電話器2の発信者番号（携帯電話番号）が発信者番号受信装置4で識別される。そして、識別された発信者番号とユーザDB5に登録されている発信者番号とが照合される。

【0025】発信者番号の照合が不一致の場合、アクセス者が登録ユーザではないとの判断の下に、アクセス拒否通知（音声データ）がサーバ3から携帯電話器2に送られる。

【0026】発信者番号の照合が一致の場合、電話回線接続の発信元である携帯電話器2（またはアクセス元のパーソナルコンピュータ1）に対しパスワードの入力が要求される。

【0027】ユーザは、入力要求に応じて、すでに確認しているパスワードを携帯電話器2から入力する。このとき、入力に使用された携帯電話器2の発信者番号が発信者番号受信装置4で識別され、その識別された発信者番号に対応するユーザIDがユーザDB5において割り出され、かつ割り出されたユーザIDに基づいてユーザDB5内のパスワード発行履歴から送信済みのパスワードが検索される。そして、検索されたパスワードと上記入力されたパスワードとが照合される。

【0028】パスワードの照合が不一致の場合、アクセス者が登録ユーザではないとの判断の下に、アクセス拒否通知（音声データ）がサーバ3から携帯電話器2に送られる。

【0029】なお、パスワードの入力受付は一定時間内に制限される。入力要求が出されてから一定時間内にパスワードが入力されなかった場合、パスワード照合が不一致の場合と同様に、アクセス拒否通知（音声データ）がサーバ3から携帯電話器2に送られる。

【0030】パスワードの照合が一致の場合は、パーソナルコンピュータ1からのアクセス者が登録者本人であるとの認証がなされ、サーバ3においてサービスの提供が許可される。同時に、許可の旨の通知（音声データ）

がサーバ3から携帯電話器2に送られる。

【0031】ユーザは、許可通知に従い、パーソナルコンピュータ1を介してホームページ画像を閲覧し、ネットワークショッピングのサービスを受けることができる。

【0032】以上のように、登録者本人を認証する要素として、ユーザID、パスワード、認証用電話番号、発信者電話番号を使用することにより、従来のようにユーザIDのみを認証に使用する場合に比べ、セキュリティ効果が大幅に向上する。

【0033】たとえば、ユーザIDが第三者に知られても、その第三者が番号登録済みの携帯電話器2または自宅電話器を持たない限り、サーバ3でのサービスを受けることは不可能であり、第三者による不正なアクセスを極力排除することができる。サービスを提供する側にとっては高い信頼性を確保することができる。

【0034】なお、ユーザIDの具体例として、携帯電話器2や自宅電話器の電話番号を使用してもよい。また、上記実施形態では、ネットワーク接続用の端末としてパーソナルコンピュータ1を用い、電話回線接続手段として携帯電話器2を用いたが、そのパーソナルコンピュータ1および携帯電話器2に代えて、ネットワーク接続の機能および電話回線接続の機能を併せ持つ複合型携帯電話器を使用してもよい。その他、この発明は上記実施形態に限定されるものではなく、要旨を変えない範囲で種々変形実施可能である。

【0035】

【発明の効果】以上述べたようにこの発明によれば、登録者本人を認証する要素として、ユーザID、パスワード、認証用電話番号、発信者電話番号を使用するようにしたので、第三者による不正なアクセスを極力排除することができるセキュリティ性にすぐれた本人認証方法および本人認証システムを提供できる。

【図面の簡単な説明】

【図1】一実施形態の構成を示すブロック図。

【図2】同実施形態の作用を説明するための図。

【符号の説明】

1…パーソナルコンピュータ（端末）、2…携帯電話器、3…サーバコンピュータ（処理装置）、4…発信者番号受信装置、5…ユーザデータベース

Figure 1 is a block diagram of the system configuration. It is divided into two main sections: 'User' (ユーザ) and 'Center' (センター).
 In the 'User' section, there is a personal computer (1) and a mobile phone (2).
 In the 'Center' section, there is a server (3), a printer/fax (4), and a database (5). The database (5) is a cylinder labeled 'ユーザDB' (User DB) and contains the following data:
 ・携帯電話番号 (Mobile phone number)
 ・ユーザID (User ID)
 ・パスワード (Password)
 ・発行履歴 (Issuance history)
 The personal computer (1) and the mobile phone (2) are connected to the server (3) via communication lines (11 and 12). The server (3) is connected to the printer/fax (4) and the database (5).

| 送 | 受 | 携帯電話 |
|-----------------------------------|------------|------------|
| 応答 | アタリ | |
| ユーザID登録確認 | ユーザID送信 | |
| 登録ユーザか？ | 表示 | |
| NO → アタリ拒否通知 | | |
| YES → アタリ拒否通知 | 表示 | |
| 「A'」コード及び認証用電話番号発行 | | |
| 携帯電話発信者番号受信 | | 認証用電話番号へ発呼 |
| 発信者番号登録確認 | | |
| 登録ユーザか？ | | 受信 |
| NO → 応答(アタリ拒否通知) | | |
| YES → 応答(「A'」要求) | | 受信 |
| 携帯番号→ユーザID →「A'」発行履歴・受信「A'」の照合 | | 「A'」入力 |
| 照合OK？ | | |
| NO → 応答(アタリ拒否通知) | | |
| YES → 「A'」許可 | | 受信 |
| | 認証完了・サービスへ | |

EE10 EE16 GG01 HH22